GSEC$^{Q\&As}$

GIAC Security Essentials Certification

Pass GIAC GSEC Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass4itsure.com/gsec.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by GIAC Official Exam Center

QUESTION 1

When trace route fails to get a timely response for a packet after three tries, which action will it take?

A. It will print \\'* * *\\' for the attempts and increase the maximum hop count by one.

B. It will exit gracefully, and indicate to the user that the destination is unreachable.

C. It will increase the timeout for the hop and resend the packets.

D. It will print \\'* * *\\' for the attempts, increment the TTL and try again until the maximum hop count.

Correct Answer: D

QUESTION 2

Which of the following areas of a network contains DNS servers and Web servers for Internet users?

A. VPN

B. MMZ

C. VLAN

D. DMZ

Correct Answer: D

QUESTION 3

Use Hashcat to crack a local shadow file. What Is the password for the user account AGainsboro?

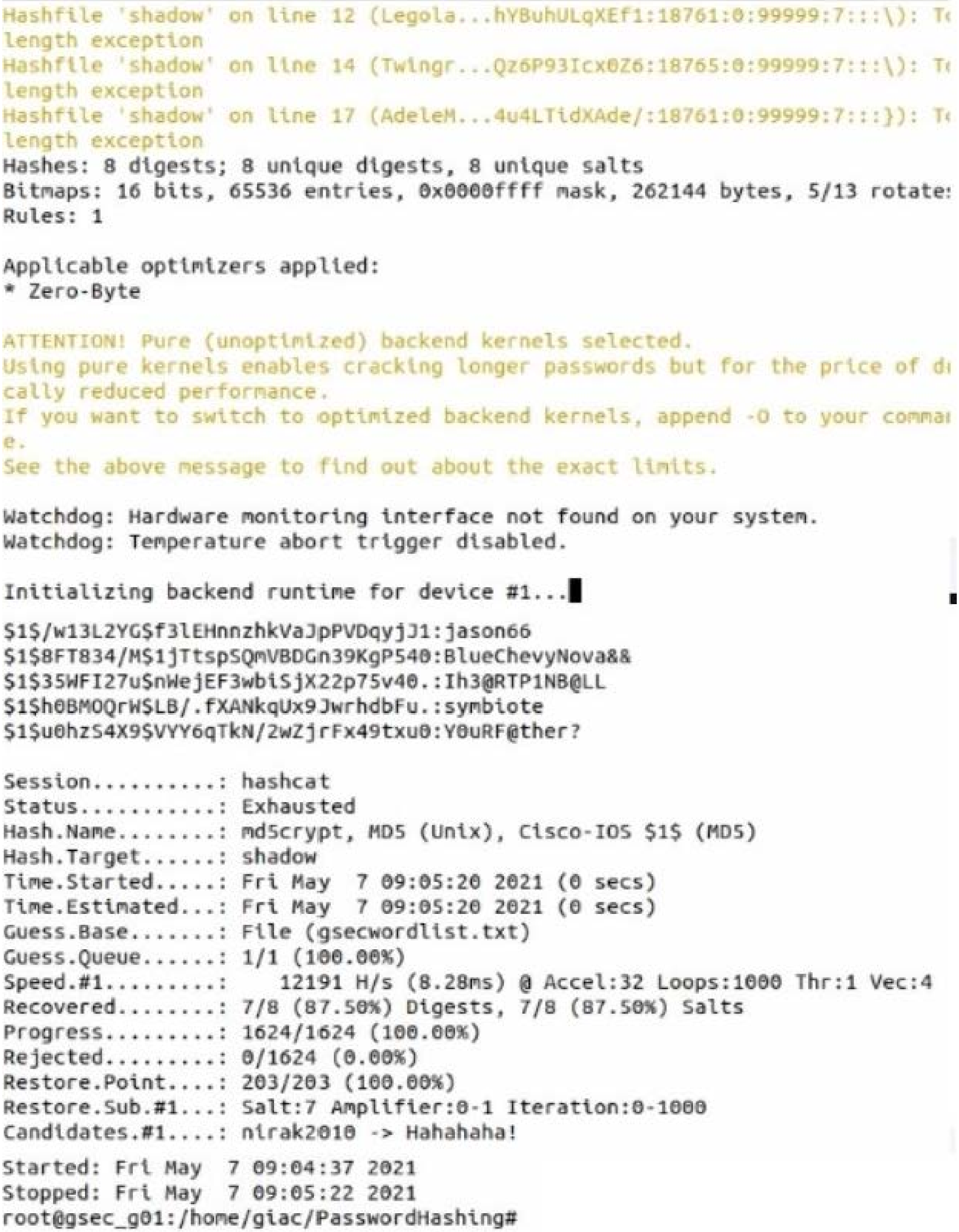
Hints

The shadow file (shadow) and Hashcat wordlist (gsecwordlist.txt) are located in the directory /home /giac /PasswordHashing/

Run Hashcat in straight mode (flag -a 0) to crack the MD5 hashes (flag -m 500) In the shadow file.

Use the hash values from the Hashcat output file and the shadow file to match the cracked password with the user name.

If required, a backup copy of the original files can be found in the shadowbackup directory.



```
Hashfile 'shadow' on line 12 (Legola...hYBuhULqXEf1:18761:0:99999:7:::\): To
length exception
Hashfile 'shadow' on line 14 (Twingr...Qz6P93Icx0Z6:18765:0:99999:7:::\): To
length exception
Hashfile 'shadow' on line 17 (AdeleM...4u4LTidXAde/:18761:0:99999:7:::}): To
length exception
Hashes: 8 digests; 8 unique digests, 8 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotate:
Rules: 1

Applicable optimizers applied:
* Zero-Byte

ATTENTION! Pure (unoptimized) backend kernels selected.
Using pure kernels enables cracking longer passwords but for the price of di
cally reduced performance.
If you want to switch to optimized backend kernels, append -O to your comma
e.
See the above message to find out about the exact limits.

Watchdog: Hardware monitoring interface not found on your system.
Watchdog: Temperature abort trigger disabled.

Initializing backend runtime for device #1...

$1$/w13L2YG$f3lEHnnzhkVaJpPVDqyjJ1:jason66
$1$8FT834/M$1jTtspSQmVBDGn39KgP540:BlueChevyNova&&
$1$35WFI27u$nWejEF3wbiSjX22p75v40.:Ih3@RTP1NB@LL
$1$h0BMOQrW$LB/.fXANkqUx9JwrhdbFu.:symbiote
$1$u0hzS4X9$VYY6qTkN/2wZjrFx49txu0:Y0uRF@ther?

Session..........: hashcat
Status...........: Exhausted
Hash.Name........: md5crypt, MD5 (Unix), Cisco-IOS $1$ (MD5)
Hash.Target......: shadow
Time.Started.....: Fri May  7 09:05:20 2021 (0 secs)
Time.Estimated...: Fri May  7 09:05:20 2021 (0 secs)
Guess.Base.......: File (gsecwordlist.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:    12191 H/s (8.28ms) @ Accel:32 Loops:1000 Thr:1 Vec:4
Recovered........: 7/8 (87.50%) Digests, 7/8 (87.50%) Salts
Progress.........: 1624/1624 (100.00%)
Rejected.........: 0/1624 (0.00%)
Restore.Point....: 203/203 (100.00%)
Restore.Sub.#1...: Salt:7 Amplifier:0-1 Iteration:0-1000
Candidates.#1....: nirak2010 -> Hahahaha!

Started: Fri May  7 09:04:37 2021
Stopped: Fri May  7 09:05:22 2021
root@gsec_g01:/home/giac/PasswordHashing#
```

A. 52345234

B. YOuRF ether?

C. symbiote

D. Volcano

E. QX689PJ688

F. LlqMM@qe

G. Noregrets2

H. Learn2Write

I. Th 3D5@60n

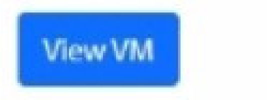
J. jason66

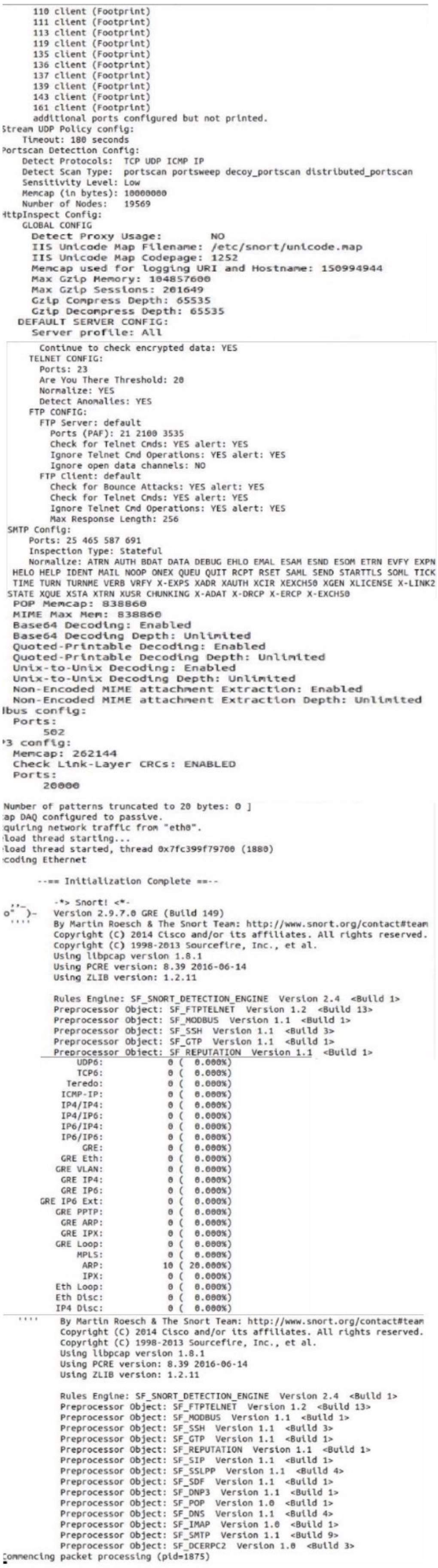
Correct Answer: E

QUESTION 4

Use sudo to launch Snort with the, /etc /snort /snort.conf file In full mode to generate alerts based on incoming traffic to echo. What is the source IP address of the traffic triggering an alert with a destination port of 156?

Note: Snort Is configured to exit after It evaluates 50 packets.





```
        110 client (Footprint)
        111 client (Footprint)
        113 client (Footprint)
        119 client (Footprint)
        135 client (Footprint)
        136 client (Footprint)
        137 client (Footprint)
        139 client (Footprint)
        143 client (Footprint)
        161 client (Footprint)
        additional ports configured but not printed.
Stream UDP Policy config:
    Timeout: 180 seconds
Portscan Detection Config:
    Detect Protocols:  TCP UDP ICMP IP
    Detect Scan Type:  portscan portsweep decoy_portscan distributed_portscan
    Sensitivity Level: Low
    Memcap (in bytes): 10000000
    Number of Nodes:   19569
HttpInspect Config:
    GLOBAL CONFIG
      Detect Proxy Usage:       NO
      IIS Unicode Map Filename: /etc/snort/unicode.map
      IIS Unicode Map Codepage: 1252
      Memcap used for logging URI and Hostname: 150994944
      Max Gzip Memory: 104857600
      Max Gzip Sessions: 201649
      Gzip Compress Depth: 65535
      Gzip Decompress Depth: 65535
    DEFAULT SERVER CONFIG:
      Server profile: All
      Continue to check encrypted data: YES
    TELNET CONFIG:
      Ports: 23
      Are You There Threshold: 20
      Normalize: YES
      Detect Anomalies: YES
    FTP CONFIG:
      FTP Server: default
        Ports (PAF): 21 2100 3535
        Check for Telnet Cmds: YES alert: YES
        Ignore Telnet Cmd Operations: YES alert: YES
        Ignore open data channels: NO
      FTP Client: default
        Check for Bounce Attacks: YES alert: YES
        Check for Telnet Cmds: YES alert: YES
        Ignore Telnet Cmd Operations: YES alert: YES
        Max Response Length: 256
SMTP Config:
    Ports: 25 465 587 691
    Inspection Type: Stateful
    Normalize: ATRN AUTH BDAT DATA DEBUG EHLO EMAL ESAM ESND ESOM ETRN EVFY EXPN
 HELO HELP IDENT MAIL NOOP ONEX QUEU QUIT RCPT RSET SAML SEND STARTTLS SOML TICK
 TIME TURN TURNME VERB VRFY X-EXPS XADR XAUTH XCIR XEXCH50 XGEN XLICENSE X-LINK2
STATE XQUE XSTA XTRN XUSR CHUNKING X-ADAT X-DRCP X-ERCP X-EXCH50
  POP Memcap: 838860
  MIME Max Mem: 838860
  Base64 Decoding: Enabled
  Base64 Decoding Depth: Unlimited
  Quoted-Printable Decoding: Enabled
  Quoted-Printable Decoding Depth: Unlimited
  Unix-to-Unix Decoding: Enabled
  Unix-to-Unix Decoding Depth: Unlimited
  Non-Encoded MIME attachment Extraction: Enabled
  Non-Encoded MIME attachment Extraction Depth: Unlimited
lbus config:
  Ports:
      502
'3 config:
  Memcap: 262144
  Check Link-Layer CRCs: ENABLED
  Ports:
      20000

Number of patterns truncated to 20 bytes: 0 ]
ap DAQ configured to passive.
quiring network traffic from "eth0".
load thread starting...
load thread started, thread 0x7fc399f79700 (1880)
coding Ethernet

        --== Initialization Complete ==--

  ,,_     -*> Snort! <*-
 o"  )~   Version 2.9.7.0 GRE (Build 149)
  ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
          Copyright (C) 2014 Cisco and/or its affiliates. All rights reserved.
          Copyright (C) 1998-2013 Sourcefire, Inc., et al.
          Using libpcap version 1.8.1
          Using PCRE version: 8.39 2016-06-14
          Using ZLIB version: 1.2.11

          Rules Engine: SF_SNORT_DETECTION_ENGINE  Version 2.4  <Build 1>
          Preprocessor Object: SF_FTPTELNET  Version 1.2  <Build 13>
          Preprocessor Object: SF_MODBUS  Version 1.1  <Build 1>
          Preprocessor Object: SF_SSH  Version 1.1  <Build 3>
          Preprocessor Object: SF_GTP  Version 1.1  <Build 1>
          Preprocessor Object: SF_REPUTATION  Version 1.1  <Build 1>
             UDP6:            0 (  0.000%)
             TCP6:            0 (  0.000%)
           Teredo:            0 (  0.000%)
          ICMP-IP:            0 (  0.000%)
          IP4/IP4:            0 (  0.000%)
          IP4/IP6:            0 (  0.000%)
          IP6/IP4:            0 (  0.000%)
          IP6/IP6:            0 (  0.000%)
              GRE:            0 (  0.000%)
          GRE Eth:            0 (  0.000%)
         GRE VLAN:            0 (  0.000%)
          GRE IP4:            0 (  0.000%)
          GRE IP6:            0 (  0.000%)
      GRE IP6 Ext:            0 (  0.000%)
         GRE PPTP:            0 (  0.000%)
          GRE ARP:            0 (  0.000%)
          GRE IPX:            0 (  0.000%)
         GRE Loop:            0 (  0.000%)
             MPLS:            0 (  0.000%)
              ARP:           10 ( 20.000%)
              IPX:            0 (  0.000%)
         Eth Loop:            0 (  0.000%)
         Eth Disc:            0 (  0.000%)
         IP4 Disc:            0 (  0.000%)
  ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
          Copyright (C) 2014 Cisco and/or its affiliates. All rights reserved.
          Copyright (C) 1998-2013 Sourcefire, Inc., et al.
          Using libpcap version 1.8.1
          Using PCRE version: 8.39 2016-06-14
          Using ZLIB version: 1.2.11

          Rules Engine: SF_SNORT_DETECTION_ENGINE  Version 2.4  <Build 1>
          Preprocessor Object: SF_FTPTELNET  Version 1.2  <Build 13>
          Preprocessor Object: SF_MODBUS  Version 1.1  <Build 1>
          Preprocessor Object: SF_SSH  Version 1.1  <Build 3>
          Preprocessor Object: SF_GTP  Version 1.1  <Build 1>
          Preprocessor Object: SF_REPUTATION  Version 1.1  <Build 1>
          Preprocessor Object: SF_SIP  Version 1.1  <Build 1>
          Preprocessor Object: SF_SSLPP  Version 1.1  <Build 4>
          Preprocessor Object: SF_SDF  Version 1.1  <Build 1>
          Preprocessor Object: SF_DNP3  Version 1.1  <Build 1>
          Preprocessor Object: SF_POP  Version 1.0  <Build 1>
          Preprocessor Object: SF_DNS  Version 1.1  <Build 4>
          Preprocessor Object: SF_IMAP  Version 1.0  <Build 1>
          Preprocessor Object: SF_SMTP  Version 1.1  <Build 9>
          Preprocessor Object: SF_DCERPC2  Version 1.0  <Build 3>
Commencing packet processing (pid=1875)
```

A. 192.168.^.30

B. 10.72.101.210

C. 10.10.28.19

D. 10.11.10.11

E. 10.10.10.66

F. 192.168.87.68

G. 10.12.10.112

H. 10.11.12.13

I. 10.10.201.150

J. 10.10.199.146

Correct Answer: I

QUESTION 5

Which of the following protocols implements VPN using IPSec?

A. SLIP

B. PPP

C. L2TP

D. PPTP

Correct Answer: C